



UNITED STATES PATENT AND TRADEMARK OFFICE

mm
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,848	02/18/2004	Michael Thomas Kurdziel	RF-235 (50589)	2513

7590 04/06/2007
CHRISTOPHER F. REGAN, ESQUIRE
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
P.O. Box 3791
Orlando, FL 32802-3791

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/780,848

Applicant(s)

KURDZIEL ET AL.

Examiner

Thomas M. Ho

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 February 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>2/18/04, 11/04/04, 6/24/05</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-26 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-8, 10-16, 18-25 rejected under 35 U.S.C. 102(e) as being anticipated by the Advanced Encryption Standard as illustrated by Stein et al. US PG PUB 2003/0133568.

In reference to claim 1:

Stein et al., US PG PUB 2003/0133568 discloses a cryptographic device comprising:

- An input stage receiving an input data block and a key data block comprising a plurality of sub-key data blocks, and generating a plurality of first signals therefrom, where the sub key data blocks are the subkeys generated for use in the AES protocol. (Figure 6)
- An intermediate stage connected to said input stage and comprising

Art Unit: 2132

- A plurality of substitution units, each substituting data within a respective first signal, where the plurality of substitution units are the units of the S-BOX substitution data block. (Figure 3) & (Figure 2, Item 16)
- A diffuser connected to said plurality of substitution units for mixing data to generate a diffused signal, where the diffuser is the SBOX substitution mechanism. (Figure 2, Item 18)
- An output stage connected to said intermediate stage for repetitively looping back the diffused signal to said input stage for combination with a next sub-key data block, where the output stage is the output of the round which is looped back into the input stage. The data signal is recombined with a next sub key data block with Item 23. (Figure 2, Items 24, 26) & (Paragraphs [0031] [0032])

In reference to claim 2:

Stein et al., US PGPUB 2003/0133568 [0031]-[0032] discloses a cryptographic device according to claim 1 wherein the looping back is repeated a predetermined number of times; and wherein said output stage provides an output signal for the cryptographic device after the repetitively looping back is complete, where the number is predetermined based on the specifics of the algorithm chosen.

In reference to claim 3:

Art Unit: 2132

Stein et al., US PG PUB 2003/0133568 [0031]-[0032] discloses a cryptographic device according to claim 2 wherein the output signal is further combined with a final sub-key data block, where the final sub-key data block is the subkey used in the last iteration.

In reference to claim 4:

Stein et al., US PG PUB 2003/0133568 [0031]-[0032] discloses a cryptographic device according to Claim 1 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table, where the non-linear substitution is the substitution performed by the lookup table. (Figure 2, Items 16, 18) & (Figure 3) & [0057]

In reference to claim 5:

Stein et al., US PG PUB 2003/0133568 [0031]-[0032] discloses a cryptographic device according to claim 1, wherein said diffuser comprises a shift register and a loop-up table associated therewith. (Figures 3, 4)

In reference to claim 6:

Stein et al., US PG PUB 2003/0133568 [0031]-[0033] discloses a cryptographic device according to claim 1 wherein said diffuser comprises a plurality of shift registers and a plurality of look-up tables associated therewith. (Figures 2, 3, 4)

In reference to claim 7:

Art Unit: 2132

Stein et al., US PGPUB 2003/0133568 [0034] discloses a cryptographic device according to claim 1 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage, where the row shift operation is a stage in the AES round. (Figure 2)

In reference to claim 8:

Stein et al., US PGPUB 2003/0133568 [0035] discloses a cryptographic device according to claim 1 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage, where the column mix operation is a stage in the AES round. (Figure 2)

Claim 10 is rejected for the same reasons as claim 2.

Claim 11 is rejected for the same reasons as claim 3.

Claim 12 is rejected for the same reasons as claim 4.

Claim 13 is rejected for the same reasons as claim 5.

Claim 14 is rejected for the same reasons as claim 6.

Claim 15 is rejected for the same reasons as claim 7.

Claim 16 is rejected for the same reasons as claim 8.

Claim 18 is rejected for the same reasons as claim 1.

Claim 19 is rejected for the same reasons as claim 2.

Art Unit: 2132

Claim 20 is rejected for the same reasons as claim 3.

Claim 21 is rejected for the same reasons as claim 4.

Claim 22 is rejected for the same reasons as claim 5.

Claim 23 is rejected for the same reasons as claim 6.

Claim 24 is rejected for the same reasons as claim 7.

Claim 25 is rejected for the same reasons as claim 8.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 9, 17, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stein et al. US PG PUB 2003/0133568.

In reference to claim 9:

Stein et al. fails to explicitly disclose a cryptographic device according to claim 1 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage.

Art Unit: 2132

Stein et al. however does disclose having an output stage loop back a given number of times to an input stage (Figure 2)

The examiner takes official notice that a counter for counting a number of times an given set of instructions is looped back into an input was well known to those of ordinary skill in the art at the time of invention.

For example, “for loops” are loops in computer science that increment a number of times until the counter equals the end condition value. At each iteration a set of instructions is executed.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a counter into order to keep track of the number of times loops in order to accurately keep track of performing a given set of instructions a set number of times.

Claim 17 is rejected for the same reasons as claim 9.

Claim 26 is rejected for the same reasons as claim 9.

Conclusion

6. The following art not relied upon is made of record:

- US Patent 6937727, disclose a method and circuit for implementing AES.
- US PGPUB 2003/0068036 discloses another circuit for implementing AES.

Art Unit: 2132

- "Cryptography and Network Security: Principles and Practice", Stallings, 2003, Chapter 5, "The Advanced Encryption Standard", pgs 140-168
- "AES proposal: Rijndael" Daemen et al. discloses the details of the Rijndael proposal, eventually accepted as the AES algorithm.

7. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov


Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

March 31st, 2007



Benjamin G. Lerner
Examiner AH 2132